

SUMS OF TWO BIQUADRATES AND ELLIPTIC CURVES OF RANK ≥ 4

F.A. IZADI, F. KHOSHNAM, AND K. NABARDI

ABSTRACT. Let n be an odd positive integer which can be written in two different ways as sums of two biquadrates. Then we show that the elliptic curve $y^2 = x^3 - nx$ has even rank ≥ 4 . If n is even number with the same property, then the curve has odd rank ≥ 3 . Moreover, some examples of ranks equal to 4, 5, 6, 7, 8 and 10, are also given.

1. INTRODUCTION

Let $E(\mathbb{Q})$ be an Elliptic curve over \mathbb{Q} defined by a Weierstrass equation of the form

$$(1.1) \quad E(\mathbb{Q}) : y^2 = x^3 + ax + b \quad a, b \in \mathbb{Q}.$$

In order the curve (1.1) to be an elliptic curve, it must be smooth. This in turn is equivalent to requiring that the cubic on the right have no multiple roots. This holds if and only if the *discriminant* of $x^3 + ax + b$, i.e., $\Delta = -(4a^3 + 27b^2)$ is non-zero.

By Mordell's theorem, the set of rational points on E is a finitely generated abelian group, i.e.,

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{tors}$ is a finite group called torsion group and r is a non-negative integer called the Mordell-Weil rank of $E(\mathbb{Q})$. In this paper, we consider the family of elliptic curves defined by

$$E_n : y^2 = x^3 - nx,$$

where n is a non-zero positive integer written in two different ways as a sums of two biquadrates.

proposition 1.1. Let $D \in \mathbb{Z}$ be a fourth -power-free integer, and let E_D be the elliptic curve

$$E_D : y^2 = x^3 + Dx.$$

Then we have

$$E_D(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{if } D = 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } -D \text{ is a perfect square,} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

Proof. See([14]. pp.311. Pro 6.1) □

Date: Februry 25, 2012.

2000 Mathematics Subject Classification. Primary 11G05; Secondary 10B10.

Key words and phrases. Elliptic curves, rank, biquadrates, sums of two biquadrates , Parity Conjecture.

As $n = p^4 + q^4$ is not -4 and can not be a square, (see for example [4], proposition 6.5.3 page 391), the curve has torsion group $T = Z/2Z$.

1.1. Previous works. Special cases of the family of the curves E_n and their ranks have been studied by many authors including Bremner and Cassels [3], Goto [6], Kudo and Motose [9], Maenishi [10], Ono and Ono [11], Spearman [15], and Hollier, Spearman and Yang [8]. The general cases were studied by Aguirre, Castaneda, and Peral [1].

Bremner and Cassels dealt with the case $n = -p$, where $p \equiv 5 \pmod{8}$ and less than 1000. The rank is always 1 in accordance with the conjecture of Selmer and Mordell.

The main result of Goto is an explicit formula for the Selmer rank of the curve E_{-n} for general $n \in \mathbb{Q}$. Kudo and Motose studied the curve for $n = p$, a Fermat or Mersenne prime and found ranks of 0 and 1. Maenishi investigated the case $n = pq$, where p, q are distinct odd primes and found a condition that the rank of E_{pq} equals 4. In Ono and Ono, the authors examined the elliptic curves given by $n = (b^2 + b)$, where $b \neq 0, -1$ is an integer. Here they show that, subject to the Parity Conjecture, one can construct infinitely many curves E_{b^2+b} with even rank ≥ 2 . Spearman takes p to be an odd prime number such that $p = u^4 + v^4$ for integers u and v and found rank equal to 1. In recent paper Spearman along with Hollier and Yang constructed elliptic curves of E_{-pq} with maximal rank 4, where $p \equiv 1 \pmod{8}$ and q be an odd prime different from p satisfying

$$q = p^2 + 24p + 400$$

Aguirre, Castaande, and Peral developed an algorithm for general n , and used it to search for curves of high rank in this family and found 4 curves of rank 13 and 22 of rank 12.

Finally, Yoshida investigated the case $n = -pq$ for distinct odd primes p and q , and showed that for general such p, q the rank is at most 5, but with additional restriction, stronger results can be proven.

1.2. Sums of two biquadrates written in two different ways. Much less is known about the equation

$$n = p^4 + q^4 = r^4 + s^4,$$

first solved by Euler. The simplest parametric solution known is

$$(1.2) \quad \begin{cases} p = a^7 + a^5b^2 - 2a^3b^4 + 3a^2b^5 + ab^6; \\ q = a^6b - 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7; \\ r = a^7 + a^5b^2 - 2a^3b^4 - 3a^2b^5 + ab^6; \\ s = a^6b + 3a^5b^2 - 2a^4b^3 + a^2b^5 + b^7; \end{cases}$$

(See Hardy and Wright[7]).

2. NEW CURVES

In this paper, we let n be a positive number which can be written in two different ways as sums of two biquadrates, i.e.,

$$n = p^4 + q^4 = r^4 + s^4,$$

where p, q, r , and s are different numbers such that $\gcd(p, q) = \gcd(r, s) = 1$. For this n , let E_n be the elliptic curve

$$y^2 = x^3 - nx.$$

We have the following main results.

Theorem 2.1. *Let n be an odd positive integer written in the forms mentioned above, then the elliptic curve: $y^2 = x^3 - nx$ subject to the Parity Conjecture has even rank ≥ 4 . If n is an even positive integer, then the curve has odd rank ≥ 3 .*

Remark 2.2. Our numerical results suggests that the odd ranks for even numbers should be at least 5.

Remark 2.3. Our results conditional on the Parity Conjecture. In [2], the authors using the previous version of our work proved the following two results unconditionally.

Theorem 1. The family $y^2 = x^3 - nx$, where $n = p^4 + q^4$ has rank at least 2 over $Q(p, q)$.

Theorem 2. The family $y^2 = x^3 - nx$, in which n given by the Euler parametrization as in part (1.2) has rank at least 4 over $Q(a)$, where a is the parameter in (1.2) and $b = 1$.

One may prove both results by a very straightforward way. For the first theorem, we note that, by the same reasons as in [2] not only the point $Q(a, b) = (-p^2, pq^2)$ but also the point $R(a, b) = (-q^2, qp^2)$ is on the curve. Then the specialization by $(p, q) = (2, 1)$ gives rise to the points $Q = (-4, 2)$ and $R = (-1, 4)$. Therefore by using the Sage software, we see that the associated height matrix has non-zero determinant 1.8567 showing that the points are independent. For the second theorem, we see that the points $Q_1(a) = (-p^2, pq^2)$, $Q_2(a) = (-q^2, qp^2)$, $Q_3(a) = (-r^2, rs^2)$, and $Q_4(a) = (-s^2, sr^2)$ are on the curve and the specialized points by $a = 2$ are given as

$$\begin{aligned} Q_1 &= (-24964, 549998, 1), Q_2 = (-3481, -1472876, 1), \\ Q_3 &= (-17956, 2370326, 1), Q_4 = (-17689, 2388148, 1). \end{aligned}$$

By using the Sage software we find that the elliptic height matrix associated to $\{Q_1, Q_2, Q_3, Q_4\}$ has non-zero determinant 5635.73654 showing that again the 4 points are independent.

Remark 2.4. We see that the map $(u, v) \rightarrow (-u^2, uv^2)$ from the quadric curve: $u^4 + v^4 = n$ to the elliptic curve: $y^2 = x^3 - nx$ takes the integral points of the first to the integrals of the second. Now to find the integral points of the quadric it is enough to find the integrals of the elliptic curves. This might suggests that to find n with more representations as sums of two biquadrates, the corresponding elliptic curves should have many independent integral points.

The Parity Conjecture takes the following explicit form (see Ono and Ono [11]). Let r be the rank of elliptic curve E_n , then

$$(-1)^r = \omega(E_n)$$

where

$$\omega(E_n) = \text{sgn}(-n)\epsilon(D) \prod_{p^2 \mid \mid D} \left(\frac{-1}{p}\right)$$

whit $p \geq 3$ a prime and

$$(2.1) \quad \epsilon(D) = \begin{cases} -1, & D \equiv 1, 3, 11, 13 \pmod{16}, \\ 1, & D \equiv 2, 5, 6, 7, 9, 10, 14, 15 \pmod{16}. \end{cases}$$

Before we give the proofs, we need the following general fact.

proposition 2.5. Let $n = u^4 + v^4 = r^4 + s^4$ be such that $\gcd(u, v) = \gcd(r, s) = 1$. If $p|n$ for an odd prime number p , then $p = 8k + 1$.

Proof. Without loss of generality we can assume that n is not divisible by 4. We use the following result from Cox [5]. Let p be an odd prime such that $\gcd(p, m) = 1$ and $p|x^2 + my^2$ with $\gcd(x, y) = 1$, then $(\frac{-m}{p}) = 1$. From one hand for $n = u^4 + v^4 = (u^2 - v^2)^2 + 2(uv)^2$, we get $(\frac{-2}{p}) = 1$ which implies that $p = 8k + 1$ or $p = 8k + 3$. On the other hand for $n = u^4 + v^4 = (u^2 + v^2)^2 - 2(uv)^2$, we get $(\frac{2}{p}) = 1$ which implies that $p = 8l + 1$ or $p = 8l + 7$. Putting these two results together we get $p = 8k + 1$. \square

Remark 2.6. If $n = p^2m$ for an odd prime p , then $p = 8k + 1$ from which we get $(\frac{-1}{p}) = 1$. This last result shows that the square factor of n does not affect the root number of the corresponding elliptic curves on the Parity Conjecture formula.

Remark 2.7. First of all, By the above remark, we have

$$\omega(E_n) = \text{sgn}(-n) \cdot \epsilon(n).$$

On the other hand, for $n = p^4 + q^4$, We note that

$$p^4 \equiv 0 \text{ or } 1 \pmod{16},$$

$$q^4 \equiv 0 \text{ or } 1 \pmod{16}.$$

For odd n we note that

$$n \equiv 1 \pmod{16}.$$

Now the Parity Conjecture implies that

$$\omega(E_n) = \text{sgn}(-n) \cdot \epsilon(n) = (-1) \cdot (-1) = 1$$

For even n we have $n \equiv 2 \pmod{16}$ and therefore $\omega(E_n) = -1$ in this case.

3. METHOD OF COMPUTATION

We use Silverman and Tate [14] to compute the rank of this family. Let G denote the group of rational points on elliptic curve E in the form $y^2 = x^3 + ax^2 + bx$. Let Q^* be the multiplicative group of non-zero rational numbers and let Q^{*2} denote the subgroup of squares of elements of Q^* . Define the group homomorphism ϕ from G to $\frac{Q^*}{Q^{*2}}$ as follows:

$$\phi(P) = \begin{cases} 1 \pmod{Q^{*2}} & \text{if } P = \mathcal{O}, \\ b \pmod{Q^{*2}} & \text{if } P = (0, 0), \\ x \pmod{Q^{*2}} & \text{if } P = (x, y) \text{ with } x \neq 0. \end{cases}$$

Similarly we take the dual curve $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ and call its group of rational points \overline{G} . Now the group homomorphism ψ from \overline{G} to $\frac{Q^*}{Q^{*2}}$ defined as

$$\psi(Q) = \begin{cases} 1 & \pmod{Q^{*2}} \text{ if } Q = \mathcal{O}, \\ a^2 - 4b & \pmod{Q^{*2}} \text{ if } Q = (0, 0), \\ x & \pmod{Q^{*2}} \text{ if } Q = (x, y) \text{ with } x \neq 0. \end{cases}$$

Then the rank r of the elliptic curve E satisfies

$$(3.1) \quad 2^{r+2} = |\phi(G)| |\psi(\overline{G})|.$$

4. PROOF OF THEOREM

Proof. First of all, we show that

$$\phi(G) \supseteq \{1, -n, -1, n\}.$$

The first two numbers 1 and $-n$ are obvious from the definition of the map ϕ . For the numbers -1 and n we note that if $n = p^4 + q^4$, then the homogenous equation

$$N^2 = -M^4 + ne^4$$

has solution $e = 1$, $M = p$, $n = q^2$. Similarly for $N^2 = nM^4 - e^4$ we have $M = 1$, $e = p$, $N = q^2$. Next, from (1.2) we see that if $-n = -(p^4 + q^4)$ then

$$\begin{aligned} -n = & -(b^4 + 6b^2a^2 + a^4)(b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8) \\ & (b^8 - 4b^6a^2 + 8b^4a^4 - 4b^2a^6 + a^8)(b^8 - b^4a^4 + a^8) \end{aligned}$$

By taking $b_1 = (b^8 + 2b^6a^2 + 11b^4a^4 + 2b^2a^6 + a^8)(b^8 - b^4a^4 + a^8)$, $M = 1$, and $e = b$ we get $N = a^2(a^6 + b^2a^4 + 4b^4a^3 - 5b^6)$. Since n is non-square, so is either b_1 or $\frac{n}{b_1} = b_2$. The corresponding point is $\left(\frac{b_1M^2}{e^2}, \frac{b_1MN}{e^3}\right)$. Since $\phi(G)$ is a subgroup of $\frac{Q^*}{Q^{*2}}$, these imply that

$$(4.1) \quad \phi(G) \supseteq \{1, -n, -1, n, b_i, -b_i\}.$$

On the other hand, for the curve

$$y^2 = x^3 + 4nx$$

we have

$$(4.2) \quad \psi(\overline{G}) \supseteq \{1, n, 2, 2n\}.$$

Again the numbers 1 and n are immediate consequence of the definition of the map ψ . For the numbers 2 and $2n$ we note that the homogeneous equation

$$N^2 = 2M^4 + 2ne^4$$

has the solution $M = (p + q)$, $e = 1$, and $N = 2(p^2 + pq + q^2)$, where $n = p^4 + q^4$. Therefore from these observations together with (3.1) we get

$$2^{r+2} = |\phi(G)| |\psi(\overline{G})| \geq 4.6$$

which implies that $r \geq 3$. But from $\omega(E_n) = 1$, the rank should be even. Therefore we see that r is even and $r \geq 4$. \square

4.1. Remark. If n is an even number n written in two different ways as sums of two biquadrates, then since $\omega(E_n) = -1$ in this case, the rank is odd and $r \geq 3$.

5. NUMERICAL EXAMPLES

We conclude this paper by providing many examples of ranks 4, 5, 6, 7, 8 and 10 using sage software [12].

TABLE 1. Curves with rank even

| p | q | n | $rank$ |
|--------|--------|-------------------------|--------|
| 114732 | 15209 | 173329443404113736737 | 10 |
| 3494 | 1623 | 155974778565937 | 8 |
| 43676 | 11447 | 3656080821185585057 | 8 |
| 500508 | 338921 | 75948917104718865094177 | 8 |
| 502 | 271 | 68899596497 | 6 |
| 292 | 193 | 8657437697 | 6 |
| 32187 | 6484 | 1075069703066384497 | 4 |
| 7604 | 5181 | 4063780581008977 | 4 |
| 133 | 134 | 635318657 | 4 |

TABLE 2. Curves with rank odd

| p | q | n | $rank$ |
|--------|--------|--------------------------|--------|
| 989727 | 161299 | 960213785093149760746642 | 7 |
| 129377 | 20297 | 280344024498199948322 | 7 |
| 103543 | 47139 | 119880781585424489842 | 7 |
| 119183 | 49003 | 207536518650314617202 | 7 |
| 3537 | 661 | 156700232476402 | 7 |
| 266063 | 72489 | 5038767537882101285602 | 5 |
| 139361 | 66981 | 397322481336075317362 | 5 |
| 38281 | 25489 | 2569595578866824162 | 5 |

REFERENCES

1. Agirre, J., Castaneda, A. and Parel, J.C. Higher rank elliptic curves with torsion group $\frac{\mathbb{Z}}{2\mathbb{Z}}$, Mathematic of Computation, Volume 73, No. 245, Pages 323-331(2003).
2. Agirre, J. and Parel, J.C. Elliptic curves and biquadrates, preprint, arXiv: 1203.2576v1.
3. Bremner, A. and Cassels, J.W.S. On the equation $Y^2 = X(X^2 + p)$, Math Comp., 42(1984), 257- 264.
4. Cohen, H. Number theory Volume I: Tools and Diophantine Equations, Springer, New York, 2007.
5. Cox, D.A. Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication (Pure and Applied Mathematics:
6. Goto, T. A note on the Selmer Group of the elliptic curve $y^2 = x^3 + Dx$, Proc. Japan Acad. Ser. A Math. Sci., 77(2001), 122-125.
7. Hardy, G.H. and Wright, E.M. An Introduction to the theory of the numbers, 4th Edition, Oxford Univ. press.
8. Hollies, A.J., Spearman, B.K. and Yang, Q. Elliptic curves $y^2 = x^3 + pqx$ with maximal rank, International Mathematical Forum, 5, 2010, No. 23, 1105-1110
9. Kudo, T. and Motose, K. On group structure of some special elliptic curves, Math. J. Okayama Univ. 47(2005), 81-84
10. Maenishi, M. On the rank of elliptic curves $y^2 = x^3 - pqx$, Kumamoto J. Math. 15(2002), 1-5.

11. Ono, K. and T. Ono, T. Quadratic form and elliptic curves III, Proc. Japan Acad. Ser. A Math. Sci. 72(1996), 204-205.
12. Sage software, *Version 4.3.5*, <http://sagemath.org>.
13. Silverman, J.H. The arithmetic of Elliptic curves, Springer, New York, 1986.
14. J.H. Silverman, J.H. and Tate, J. Rational points on elliptic curves, Springer, New York, 1985.
15. Spearman, B.K, Elliptic curves $y^2 = x^3 - px$, Math. J. Okayama Univ. 49(2007), 183-184
16. Yoshida, S. On the equation $y^2 = x^3 + pqx$, Comment. Math. Univ. St. Paul., 49(2000), 23-42.

MATHEMATICS DEPARTMENT AZARBAIJAN UNIVERSITY OF TARBIAT MOALLEM , TABRIZ, IRAN
E-mail address: **f.izadi@utoronto.ca**

MATHEMATICS DEPARTMENT AZARBAIJAN UNIVERSITY OF TARBIAT MOALLEM , TABRIZ, IRAN
E-mail address: **khoshnam@azaruniv.edu**

MATHEMATICS DEPARTMENT AZARBAIJAN UNIVERSITY OF TARBIAT MOALLEM , TABRIZ, IRAN
E-mail address: **nabardi@azaruniv.edu**